

## CLAIMS

1. An authentication server that detects an unauthorized terminal in terminals that accessed the authentication server via a network, comprising:

a terminal information receiving unit operable to receive, from a terminal, authentication data generated based on a terminal key that is previously given to the terminal and a terminal ID that is identification information assigned to said each manufactured terminal;

a terminal key verification unit operable to verify authenticity of the terminal key using the received authentication data;

a terminal information search unit operable to previously hold predetermined terminal information concerning a plurality of terminal and try to search the received terminal ID based on the terminal information; and

an unauthorized terminal determination unit operable to determine that the terminal is an unauthorized terminal in the case where the terminal key verification unit verifies the authenticity of the terminal key, but the terminal key verification unit detects a terminal ID different from the received terminal ID.

2. The authentication server according to Claim 1, further comprising:

a receiving unit operable to receive the terminal ID from an operator of the authentication server; and

an unregistered terminal ID determination unit operable to determine whether the received terminal ID is registered in terminal information stored in the terminal information search unit,

wherein the terminal information search unit further

registers the terminal ID in the case where the authenticity of the terminal key is verified and the unregistered terminal ID determination unit judges that the terminal ID is not registered.

- 5     3.     The authentication server according to one of Claim 1 and Claim 2,

          wherein, the terminal is permitted to access the digital content related to a predetermined package content at predetermined times by accessing the authentication server via  
10   the network,

          the authentication server further comprising  
          a history storage unit operable to store information indicating history of a digital content that is accessed by the terminal for said each terminal specified by a pair of the terminal  
15   key and the terminal ID,

          wherein the unauthorized terminal judgment unit further judges that the terminal is an unauthorized terminal in the case where a digital content that is accessed exceeding the access limit from a terminal that has an identical terminal key and an identical  
20   terminal ID.

4.     The authentication server according to Claim 3,  
          wherein the terminal key is a secret key in a secret key encryption method or a public key certificate in a public key  
25   encryption method.

5.     An unauthorized terminal detection system comprising an authentication server that detects an unauthorized terminal in terminals that accessed the authentication server via a network  
30   and a terminal that can access the authentication server via a network,

          wherein the terminal includes

a terminal information sending unit operable to send, to the authentication server, authentication data generated based on a terminal key that is previously given to the terminal and a terminal ID that is identification information assigned to said each  
5 manufactured terminal,

the authentication server includes:

a terminal information receiving unit operable to receive, from the terminal, authentication data generated based on the terminal key and the terminal ID;

10 a terminal key verification unit operable to verify authenticity of the terminal key using the received authentication data;

a terminal information search unit operable to previously hold predetermined terminal information concerning a plurality of  
15 terminals and try to search the received terminal ID; and

an unauthorized terminal determination unit operable to determine that the terminal is an unauthorized terminal in the case where the terminal key verification unit verifies the authenticity of the terminal key, but the terminal key verification unit detects a  
20 terminal ID different from the received terminal ID.

6. An unauthorized terminal detection method for detecting an unauthorized terminal in terminals that accessed the authentication server via a network, comprising:

25 receiving, from the terminal, authentication data generated based on a terminal key that is previously given to the terminal and a terminal ID that is identification information assigned to said each manufactured terminal;

30 verifying authenticity of the terminal key using the received authentication data;

trying to search the received terminal ID based on the held predetermined terminal information concerning a plurality of

terminal; and

determining that a terminal is an unauthorized terminal in the case where the authenticity of the terminal key is verified in the verifying, but a terminal ID different from the received terminal ID is detected.

7. The unauthorized terminal detection method according to Claim 6, further comprising:

receiving a terminal ID from an operator; and

determining whether the received terminal ID is registered in the held terminal information,

wherein, further, the authenticity of the terminal key is verified, and a terminal ID is registered in the case where it is judged in the determining that the terminal ID is not registered.

8. A program for an authentication server that detects an unauthorized terminal in terminals that accessed the authentication server via a network, the program causing a computer to execute:

receiving, from the terminal, authentication data generated based on a terminal key that is previously given to the terminal and a terminal ID that is identification information assigned to said each manufactured terminal;

verifying authenticity of the terminal key using the received authentication data;

trying to search the received terminal ID based on the held predetermined terminal information concerning a plurality of terminals; and

determining that the terminal is an unauthorized terminal in the case where the authenticity of the terminal key is verified in the verifying, but a terminal ID different from the received terminal ID is detected.

9. The program according to Claim 8, further comprising:  
receiving a terminal ID from an operator; and  
determining whether the received terminal ID is registered  
in the held terminal information,

5 wherein, the authenticity of the terminal key is verified and  
a terminal ID is registered in the case where it is judged in the  
determining that the terminal ID is not registered.

10